(E) ISSN: 3030-3214
Volume 3, № 2
2025

UO‘K: 004.056.55:004.942:519.876 10.70769/3030-3214.SRT.3.2.2025.3

IOT TRAFIK FRAKTAL O‘LCHOVINING STATISTIK XUSUSIYATLARI: KITSUNE MA’LUMOTLAR TO‘PLAMI MISOLIDA



Majidov Anvarxon Mahmudxon o‘g‘li
O‘zbekiston Milliy Unversiteti Axborot xavfsizligi magistranti, Toshkent, O‘zbekiston
Email: anvarxonmajidov2000@gmail.com

Annotatsiya. *Ushbu maqola trafikning fraktal xususiyatlarini baholash usulini ko‘rib chiqadi va IoT trafikining fraktal o‘lchovining statistik parametrlarini baholaydi. Kitsune to‘plamidan hujumlar bilan birga real trafik tahlili, shuningdek, normal holatda va SSDP Flood, Mirai, OS Scan kabi hujumlar ta’sirida trafikning fraktal xususiyatlari tahlil qilingan. Natijalar shuni ko‘rsatdiki, hujum paytida trafikning fraktal o‘lchovidagi keskin o‘zgarishlar IoT tarmoqlaridagi kompyuter hujumlarini aniqlash algoritmlarini yaratish uchun ishlatilishi mumkin. Tadqiqotlar shuni ko‘rsatdiki, tarmoq trafiklarini onlayn tahlil qilganda fraktal o‘lcham (FR)ni baholashda sirpanuvchi tahlil oynasida Hurst ko‘rsatkichini baholash uchun modifikatsiya qilingan algoritm afzalroqdir.*

Kalit so‘zlar: *Hurst ko‘rsatkichi, fraktal o‘lchov, chegaralash, kompyuter hujumi, tarmoq trafiklari, narsalar interneti (IoT).*

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ФРАКТАЛЬНОЙ РАЗМЕРНОСТИ ТРАФИКА IOT: ПРИМЕР НА ОСНОВЕ ДАТАСЕТА KITSUNE

Маджидов Анвархон Махмудхон угли
Степень магистра по специальности «Информационная безопасность», Национальный университет Узбекистана, Ташкент, Узбекистан

Аннотация. *В статье рассматривается метод оценки фрактальных характеристик сетевого трафика и анализируются статистические параметры фрактальной размерности IoT-трафика. Проведен анализ реального трафика вместе с атаками из набора данных Kitsune, а также изучены фрактальные свойства трафика в нормальных условиях и при атаках, таких как SSDP Flood, Mirai и OS Scan. Результаты показывают, что резкие изменения фрактальной размерности трафика во время атак могут быть использованы для создания алгоритмов обнаружения кибератак в IoT-сетях. Исследование демонстрирует, что модифицированный алгоритм оценки индекса Хёрста в скользящем окне анализа является предпочтительным для оценки фрактальной размерности при онлайн-анализе сетевого трафика.*

Ключевые слова: *показатель Херста, фрактальная размерность, пороговая обработка, кибератака, сетевой трафик, интернет вещей (IoT).*

STATISTICAL CHARACTERISTICS OF IOT TRAFFIC FRACTAL DIMENSION: A CASE STUDY OF THE KITSUNE DATASET

Majidov Anvarkhan Makhmudkhan ugli
Master's degree in Information Security, National University of Uzbekistan, Tashkent, Uzbekistan

Abstract. *This article examines a method for evaluating the fractal characteristics of traffic and assesses the statistical parameters of the fractal dimension of IoT traffic. It analyzes real traffic alongside attacks from the Kitsune dataset, as well as the fractal properties of traffic under normal conditions and during attacks such as SSDP Flood, Mirai, and OS Scan. The results indicate that abrupt changes in the fractal dimension of traffic during attacks can be utilized to develop algorithms for detecting cyberattacks in IoT networks. The research demonstrates that a modified algorithm for estimating the Hurst index within a sliding analysis window is preferable for evaluating the fractal dimension during online analysis of network traffic.*
Keywords: *Hurst exponent, fractal dimension, thresholding, cyberattack, network traffic, Internet of Things (IoT).*

Kirish. Narsalar interneti (IoT, inglizcha “Internet of Things”) texnologiyalari nisbatan yangi paydo bo‘lgan va oxirgi o‘n yil ichida keng tarqalgan. IoT — bu bir-biri bilan bog‘langan kompyuter tarmoqlari va ko‘plab o‘rnatilgan sensorlar bilan jihozlangan fizik obyektlar sistemasini ifodalaydi. Bu sensorlar atrof-muhit haqidagi ma’lumotlarni yig‘ish uchun ishlatiladi. Ma’lumotlarni qayta ishlash va datchiklardan keladigan ma’lumotlarni keyingi tahlil, masofaviy monitoring va IoT obyektlarini foydalanuvchi ishtirokisiz boshqarish uchun maxsus dasturiy ta’minotdan foydalaniladi. Bundan tashqari, dasturiy ta’minot ma’lumotlarni saqlash va ularga kirish imkonini ta’minlaydi [1, 2]. Odatda IoT doirasida har biriga alohida vazifalar uchun mo‘ljallangan alohida tarmoqlar mavjud.

IoT sohasidagi mutaxassislarning bashoratlariga ko‘ra, 2020-yildan 2025-yilgacha “aqlli” qurilmalar soni har yili 20% ga ortib boradi [3]. Qurilmalar sonining tez o‘sishi va texnologiya rivojlanishi bilan axborot xavfsizligini ta’minlashga oid risklar ham ortmoqda. IoT qurilmalari (internetga ulangan “aqlli” uy jihozlari) internetga ulangan holda bir-biri bilan bog‘liq bo‘lib, ko‘pincha zararli foydalanuvchilar tomonidan ushbu qurilmalarning resurslariga kirish uchun hujumning maqsadiga aylanadi.

IoT qurilmalari cheklangan xotira hajmi va past hisoblash quvvatiga ega bo‘lgani sababli, ularda tarmoq xavfsizligini ta’minlovchi vositalar odatda o‘rnatilmaydi. Bunday zaifliklardan foydalanib, zarrarli dasturlar yordamida botnetlar IoT qurilmalarini nazorat ostiga olish va boshqarish imkoniyatiga ega bo‘ladi. Eng mashhur zararli dasturlardan biri Miraidir. Masalan, Mirai botnetining bir versiyasi dunyoning 164 mamlakatida joylashgan 5 milliondan ortiq qurilmaga, shu jumladan IoT qurilmalariga kirish huquqini olishga muavvaffaq bo‘lgan. Bu oiladagi zararli dasturlar barcha hujumlarining 39% ini tashkil etadi. IoT tarmoqlaridagi eng keng tarqalgan boshqa hujumlar SSDP Flood va OS Scan turidagi hujumlar hisoblanadi. SSDP Flood – bu tarmoqdagi UPnP xizmatidan foydalanib amalga oshiriladigan DDoS hujumi. OS Scan – bu operatsion tizimni aniqlash va zaifliklarni topish uchun ishlatiladigan tahlil usuli.

Adabiyotlar tahlili va metodologiya. Tarmoq trafikining xavfsizlikni ta’minlash vositalarini yaratish asosi sifatida ishlatilishi mumkin bo‘lgan muhim parametrlaridan biri uning fraktal xususiyatlaridir. Ma’lumki, tarmoq trafiki o‘z-o‘ziga o‘xshashlik yoki fraktal xususiyatlarga ega [6, 7]. Fraktal xususiyatlarni miqdoriy baholash uchun asosan Hurst ko‘rsatkichi H ishlatiladi, bu ko‘rsatkich fraktal o‘lchov (FR) D bilan quyidagi munosabat orqali bog‘langan: $D = 2 - H$ [8–10] ishlarida ko‘rsatilganidek, Hurst ko‘rsatkichiga asoslanib, quyidagi statistik xarakteristikalarga ega bo‘lgan tarmoq trafikining normal faoliyatini aniqlash mumkin:

1) Tanlangan o‘rtacha qiymat;

$$M_{H,i} = \frac{1}{n}\sum_{j=i}^{i+n} S_j \; ; \qquad (1)$$

2) Tanlab olingan dispersiya. Tanlab olingan dispersiya quyidagicha hisoblanadi:

$$D_{H,i} = \frac{1}{n-1}\sum_{j=i}^{i+n} (S_j - M_{H,i})^2 \; ; \qquad (2)$$

3) Assimetriya koeffitsienti. Hurst ko‘rsatkichining ehtimollik zichlik taqsimotining markaziy og‘irlik o‘qiga nisbatan assimmetrikligini aniqlovchi quyidagi formulaga asoslanadi:

(E) ISSN: 3030-3214
Volume 3, № 2
2025

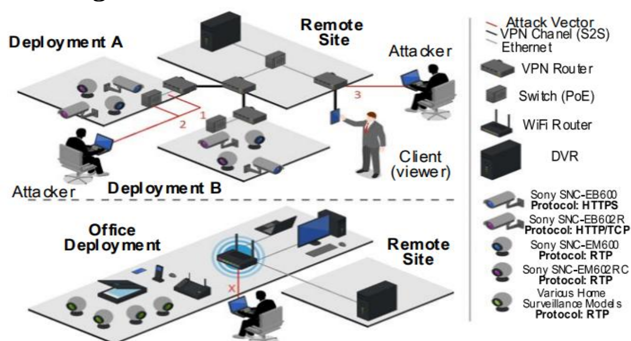
$$\gamma_{H1,i} = \frac{\frac{1}{n-1} \quad \sum_{j=i}^{i+n}(S_j - M_{H,i})^2}{D_{H,i}}; \qquad (3)$$

4) Ekstsess koeffitsienti. Hurst ko‘rsatkichining ehtimollik taqsimotining qattiq uchini normal taqsimot bilan solishtirib, quyidagi formulaga asoslanadi:

$$\gamma_{H2,i} = \frac{\frac{1}{n-1}\sum_{j=i}^{i+n}(S_j - M_{H,i})^4}{D^2{}_{H,i}} - 3. \qquad (4)$$

Ushbu parametrlar tarmoq himoyasini samarali tizimini qurishda, ma’lumotlarni intellektual tahlil qilish [11, 12] va fraktal tahlil usullariga asoslanib ishlatilishi mumkin. Ishning maqsadi – IoT tarmog‘idagi eng keng tarqalgan hujumlarning fraktal o‘lchov statistik xususiyatlarini o‘rganish, va Kitsune ma’lumotlar bazasi asosida tahlil qilish.

IoT trafikining fraktal o‘lchov statistik parametrlarini baholashni Kitsune ma’lumotlar bazasi [13−15] asosida amalga oshiramiz. Kitsune – bu sun’iy neyron tarmog‘iga (ANN), asoslangan tarmoqdagi kirishlarni aniqlash tizimi (NIDS), avtomatik tarzda onlayn ishlaydigan tizimdir. 1-rasmda taqdim etilgan tarmoq topologiyasi asosida tarmoq trafikini 1, 2, 3 va X nuqtalaridagi routerlar orqali ushlab olish amalga oshirilgan. Har bir ma’lumotlar to‘plami uchun avval bir million paketli sof trafik ushlanib, keyin hujum amalga oshirilgan. Illyustratsiyada hujum vektorlar ham ko‘rsatilgan.



1-rasm. Tarmoq topologiyasi.

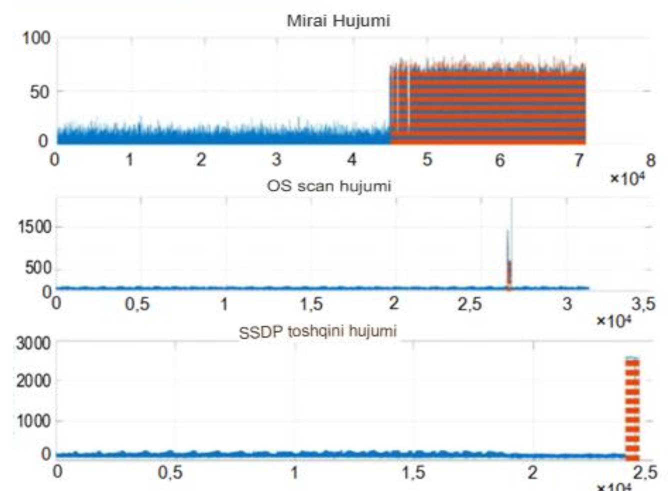
Obyektlarni chiqarish strukturasini AfterImage deb atashadi, bu har bir tarmoq kanalining shablonlarini samarali kuzatib boradi, kamayib boruvchi statistik ma’lumotlar yordamida va har bir paket uchun xususiyatlar vektorini chiqarib oladi. Ushbu vektor kanal va paket yuboruvchisi vaqt kontekstini qayd etadi. Kuzatilgan obyektlar ko‘rinadigan neyronlar githubdagi Kitsune guruhiga joylashtiriladi.

Kitsune ma’lumotlar bazasi 2019 yilda ochiq bo‘lib, eng yirik haqiqiy va model asosidagi mashina o‘rganish vazifalari saqlanadigan UCI Machine Learning Repository protokoli repozitoriyasiga kiritildi. U to‘rt xil hujum turini o‘z ichiga oladi: razvedka (Recon), odam o‘rtada (MitM), xizmat ko‘rsatishni rad etish (DoS) va botnet zararli dasturlari (Botnet Malware), masalan, Mirai – bu IoT qurilmalarini, ayniqsa ARC protsessorlarida ishlaydiganlarini, zararli dastur bilan yuqtirib, ulardan masofadan boshqariladigan botlar tarmog‘ini yaratadi. Ushbu botnet ko‘pincha DDoS-hujumlarini amalga oshirish uchun ishlatiladi.

Hujumlar haqidagi ma’lumotlar tijorat IP-nazorat tizimi va IoT qurilmalarini o‘z ichiga olgan tarmoqdan olingan. Har bir ma’lumotlar to‘plami millionlab tarmoq paketlari va turli xil kiberhujumlarni o‘z ichiga oladi. Har bir hujum turi uchun quyidagi ma’lumotlar to‘plami mavjud:

– oldindan ishlov berilgan ma’lumotlar to‘plami, bu mashina o‘rganish algoritmlarini qo‘llash uchun tayyor, .csv formatida;
– belgilash fayli (.csv formatida);
– asl tarmoq tarmog‘ini ushlash fayli .pcap formatida.

1-jadvalda Kitsune ma’lumotlar bazasida mavjud bo‘lgan tarmoq hujumlarining turlari ko‘rsatilgan. Tadqiqotda IoT trafikining fraktal xususiyatlari tahlil qilingan va hujumlar bo‘yicha tahlil qilingan: SSDP Flood (54 soniya davomida), Mirai (44 daqiqa davomida), OS Scan (29 soniya davomida), 2-rasmda ko‘rsatilgan.



2-rasm. IoT trafik, Normal trafik (ko‘k), Hujum trafik (qizil).

(E) ISSN: 3030-3214
Volume 3, № 2
2025

Fraktal xususiyatlarni baholash uchun 100 ms interval bilan harakatlanuvchi oynada ushlangan paketlar tarmog‘ining tahlili amalga oshirilgan. 2-jadvalda oldindan ishlov berilgan ma’lumotlar to‘plami va asl tarmoq tarmog‘ini ushlash faylini (pcap formatida) ko‘rsatuvchi tegishli belgilash vektori keltirilgan.

Har bir .csv-fayl satri ushlangan va ishlov berilgan paketni ifodalaydi va uning vaqt statistikasi haqida ma’lumotlarni o‘z ichiga oladi. Bu ma’lumotlar paketning uzatilish kontekstini tasvirlab beradi, shu jumladan, uzatilishda ishtirok etgan hostlar va protokollar haqida ma'lumotlarni. Ushbu ma’lumotlar 115 xil turdagi statistik ma’lumotni (atribut) o‘z ichiga oladi va ular paket yuboruvchisi va qabul qiluvchisi orasidagi tarmoqni tavsiflaydi. Statistika yig‘ish barcha trafik uchun amalga oshirilgan bo‘lib, manba sifatida paketning MAC- va IP- manzillari (SrcMAC-IP) ishlatilgan. Tahlil qilish uchun qo‘shimcha ma’lumot sifatida paketning manba IP-manzili (SrcIP) ham ishlatilgan. Agar paketning uzatish kanali tahlil qilinayotgan bo‘lsa, u holda kanal nomi bilan belgilangan paketning manba va maqsad IP-manzillari o‘rtasidagi bog‘lanishni o‘rganish mumkin. Tarmoq aloqalari (Socket)ni o‘rganish uchun esa TCP/UDP protokollarining soket ma’lumotlari ishlatilgan. Bir vaqt o‘ynasidan chiqariladigan umumiy atributlar soni 23 ni tashkil qiladi. Atributlarni chiqarish uchun turli uzunlikdagi beshta tahlil oynasi ishlatiladi: 100 ms, 500 ms, 1,5 soniya, 10 soniya va 1 daqiqa. Bular birgalikda 115 atributni hosil qiladi. Agar TCP/UDP protokolida ma’lumotlar mavjud bo‘lmasa, mos funksiyalar nolga tenglashtiriladi.

1-jadval

Hujum haqida ma’lumotlar

Hujum turi	Hujum nomi	Tavsif	Hujum vektori	Paket soni	Davomiyligi, minut
Recon	OS Scan	Hujumchi tarmoqdagi hostlarni va ularning operatsion tizimlarini skanerlaydi, potentsial zaifliklarni aniqlashga urinadi.	1	1 697 851	52,2
	Fuzzing	Hujumchi veb-serverlardagi kameralarning zaifliklarini tasodifiy buyruqlar yuborib skanerlaydi.	3	2 244 139	85,5
Man in the Middle	Video Injection	Zararli shaxs yozilgan videoni umumiy video oqimiga kiritadi.	1	2 472 401	33,4
	ARP MitM	Zararli shaxs ARP-hujumi orqali barcha LAN-trafikni uzatib oladi.	1	2 504 267	28,2
	Active Wiretap	Zararli shaxs ochiq sim orqali o‘rnatilgan faol tinglash (tarmoq ko‘prigi) orqali barcha tarmoq trafiklarini uzatib oladi.	2	4 554 925	95,6
Denial of Service	SSDP Flood	Zararli shaxs videoregistratorni reklama e‘lonlari serveriga spam tarqatish uchun kameralarni majburlaydi	1	4 077 266	40,8
	SYN DoS	Zararli shaxs uning veb-serverini yuklab tashlab, kameraning video oqimini o‘chiradi.	1	2 771 276	52,8
	SSL Renegotiation	Zararli shaxs kameralarga ko'plab SSL-qayta kelishuv paketlarini yuborib, uning video oqimini o'chiradi.	1	6 084 492	65,6
Botnet Malware	Mirai	Zararli shaxs IoT qurilmalarini standart kirish ma'lumotlaridan foydalanib Mirai zararli dasturi bilan zararlaydi va keyin yangi zaif tarmoqni skanerlaydi.	X	764 137	118,9

2-jadval

Kitsune ma’lumotlar to‘plamining xarakteristikasi

Hujum turi	Hujum nomi	Paket soni
Botnetlar uchun zararli dasturiy ta’minot	Mirai	764 136
Xizmat ko‘rsatishni rad etish	SSL Renegotiation	2 207 570
	SSDP Flood	4 077 265
	SYN DoS	2 771 275
O‘rta qismda odam	ARP MitM	2 504 266
	Video iny’eksiya	2 472 400
	Faol tinglash	2 278 688
Razvedka	Operatsion tizimlarni skanerlash	1 697 850
	Fuzzing	2 244 138

Natijalar. Fraktal o‘lchamni tavsiflovchi Hrust ko‘rsatkichini baholash uchun eng ko‘p qo‘llaniladigan usullarga normallashtirilgan tahlili (R/S-usuli), dispersiya o‘zgarishining grafigi va wveivlet-tahlil kiradi [6, 7].

R/S-usulidan foydalanilganda, berilgan kuzatuvlar to‘plami X uchun o‘rta qiymat quyidagicha aniqlanadi:

$$\bar{X} = \frac{1}{n}\sum_{j=1}^{n} X_j \,, \qquad (5)$$

bu yerda n - kuzatuvlar soni, shu bilan birga, yoyilma tushunchasi kiritiladi, bu esa maksimal va minimal og‘ishlar orasidagi farqdir:

$$R(n) = \max \Delta_j - \min \Delta_j, \qquad (6)$$

bu yerda $1 \leq j \leq n;\ \Delta_k = \sum_{i=1}^{k}(X_i - k\bar{X});\ \forall k = \overline{1, n},$

(E) ISSN: 3030-3214
Volume 3, № 2
2025

$$S(n) = \frac{1}{n}\sum_{j=1}^{n}(X_j - \bar{X})^2 \ . \qquad (7)$$

Ko‘plab tabiiy hodisalar uchun normallashtirilgan yoyilmaning matematik kutilishi taxminan quyidagiga teng bo‘ladi: $CnH \ n \to \infty$, bu yerda C ga bog‘liq bo‘lmagan musbat konstanta. Natijada, Hurst ko‘rsatkichi H qiymatini baholash uchun quyidagi logarifmik bog‘liqlik grafigi quriladi:

$$\log(M\frac{R(n)}{S(n)}) \ dan \ \log(n), \qquad (8)$$

Grafikda olingan nuqtalar asosida eng kichik kvadratlar usuli orqali to‘g‘ri chiziq yasaladi, uning burchak koeffitsienti H ni ifodalaydi [6, 7].

Hurst ko‘rsatkichining miqdoriy qiymatini aniqlash uchun quyidagi munosabatdan foydalaniladi:

$$H = \frac{\ln(R/S)}{\ln(n/2)}. \qquad (9)$$

Haqiqiy vaqtda FR baholash uchun o‘lchov oynasi uzunligi L bo‘lgan Hurst ko‘rsatkichining baholash usuli qo‘llaniladi. Keskin o‘zgarishlarni neytrallash va buzilish dispersiyasini kamaytirish uchun [9] ishida thresholding (chegaraviy qiymatlash) jarayonidan foydalanish taklif etilgan.

Thresholding – bu shovqinlardan signallarni tozalashga qaratilgan, veivlet almashtirishiga asoslangan usuldir. Thresholdingdan foydalanish natijasida Hurst ko‘rsatkichining joriy bahosi uchun formula quyidagi ko‘rinishga ega bo‘ldi [9, 10]:

$$H(t_m) = \sum_{l=1}^{L_0} a_l{}^{(H)}\varphi_l{}^{(H)}(t_m) + \sum_{j=1}^{J}\ \sum_{l=1}^{L_j} T(d_{j,l}{}^{(H)})\Psi_{j,l}{}^{(H)}\,(t_m), \qquad (10)$$

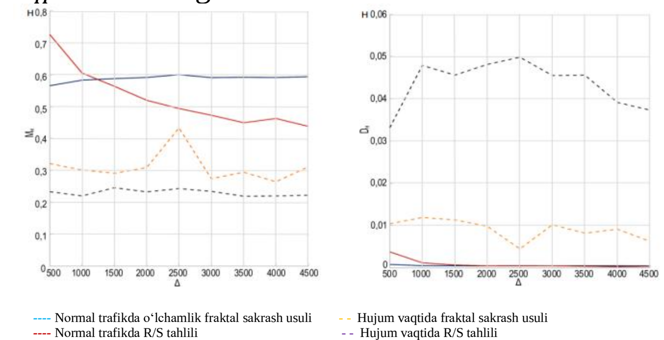
$\varphi_l{}^{(H)}(t_m)$ va $\Psi_{j,l}{}^{(H)}(t_m)$ – bazisli masshtablash va veivlet-funksiyalar; $a_{j_0,l}{}^{(H)}$va $d_{j,l}{}^{(H)}$ – Hurst ko‘rsatkichining approksimatsiya va detalizatsiya koeffitsientlari, m-oynaning filtratsiya holatida hisoblanadi; $T(d_{j,l}{}^{(H)})$ – thresholding (chegaraviy qiymatlash) yordamida filtrlangan detalizatsiya veivlet-koeffitsientlari; $L_0 = 2Jmax$, $(L_0 \leq L)$; $Jmax = \log_2 L$ – parchalanishning maksimal masshtablar soni; [log2 L] – sonning butun qismi; masshtab approksimatsiya koeffitsienti $a_{j_0,l}{}^{(H)}$; Hurst ko‘rsatkichining bahosi $\widehat{H}(t_m)$ va eng katta masshtabdagi $\varphi_l{}^{(H)}$ masshtab funksiyasining skalyar ko‘paytmasiga teng bo‘lib, u l masshtab birligiga o‘ngga siljigan holda quyidagicha aniqlanadi:

$$a_{j_0,l}{}^{(H)} = \langle \widehat{H}(t_m), \varphi_l{}^{(H)} \rangle; \ (11)$$

Detalizatsiya veivlet-koeffitsienti $d_{j,l}(H)$, Hurst ko‘rsatkichining bahosi $\widehat{H}(t_m)$ va j masshtabli $\psi j(H,l)$ veivletining skalyar ko‘paytmasiga teng bo‘lib, u l masshtab birligiga o‘ngga siljigan holda quyidagicha aniqlanadi:

$$d_{j,l}{}^{(H)} = \langle \widehat{H}(t_m), \Psi_{j,l}{}^{(H)} \rangle, \qquad (12)$$

(11) va (12) formulalaridan foydalanib IoT trafikining eksperimental ma’lumotlarini qayta ishlash natijasida Hurst ko‘rsatkichining statistik xarakteristikalari olingan. 3-rasmda normal trafik va Mirai hujumi ostidagi trafik uchun hisoblangan fraktal o‘lchamning statistik parametrlari – M_H va D_H – tasvirlangan.



3-rasm. Indikator H ning statistik parametrlari va ularning normal IoT trafik oynasi (dump) hamda Mirai hujumi ostidagi analiz oynasi o‘lchamiga bog‘liqligi:
a) M_H – chapda; b) D_H – o‘ngda.

Taqqoslash tahlili ko‘rsatilgan bog‘lanishlarning natijalarini taqdim etadi va R/S metodini hamda wavelet-analizini qo‘llash orqali olinadigan statistik xususiyatlarni baholashda olingan natijalar asosan bir xil ekanligini ko‘rsatadi. M_H uchun tarqalish taxminan 0.1 ga teng, D_H esa 0.03 dan oshmaydi. Baholashdagi farqlar wavelet-analizida harakatchan baholash usuliga bog‘liq. 4-rasmdagi Hurst ko‘rsatkichining taqsimlanishi gistonogrammasini sharhlash uchun, olingan natijalarni sifatli tahlil qilish shuni ko‘rsatadiki, Mirai hujumi ta’sirida IoT trafiki Hurst ko‘rsatkichi $0 < H < 0.5$ oraliqda bo‘ladi. Bu esa tahlil qilinayotgan tasodifiy jarayonning o‘zini-o‘zi o‘xshatish (self-similarity) xususiyatiga ega emasligini bildiradi.

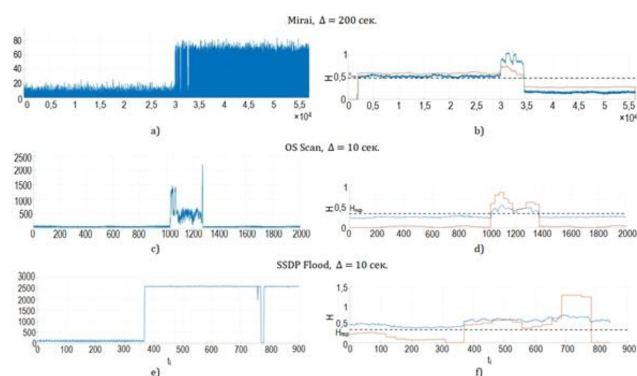
Boshqa tomondan, 3- va 4-rasmlardan ko‘rinib turibdiki, hujumlar bo‘lmagan holatda trafik fraktal xususiyatlarga ega bo‘lib, bu xususiyatlar

(E) ISSN: 3030-3214
Volume 3, № 2
2025

tarmoqlardagi hujumlarni aniqlash algoritmlari asosiga qo‘yilishi mumkin. 5-rasmda esa Hurst ko‘rsatkichining slayd oynasida hisoblangan bahosi ko‘rsatilgan bo‘lib, yuqorida ko‘rilgan ikkita baholash algoritmi yordamida aniqlangan. Mirai hujumi, Hurst ko‘rsatkichining joriy bahosi belgilangan H_{pop} qiymatidan oshganida aniqlanishi mumkin (5a va 5b rasmlarni qarang). 5c-5d- rasmlarda esa OS Scan hujumi uchun ikkita baholash algoritmi yordamida Hurst ko‘rsatkichining joriy bahosi ko‘rsatilgan.

4-rasm. Normal IoT trafik oynasi (dump) va Mirai hujumi uchun $\Delta = 200$ sekund dagi Hurst koeffitsientining taqsimoti quyidagi algoritm yordamida hisoblangan:

a) Fraktal o‘lchovning oshib borishini aniqlash usuli chegaralash bilan; b) R/S tahlili.



5-rasm. IoT trafikni (1) va (2) algoritmlari yordamida H baholash:

a), c), e) hujum bilan trafik fragmenti; b), d), f) – sirpanuvchi oyna ichida Hurst koeffitsientining baholashi.

5c va 5d rasmlarda ko‘rsatilgan Hurst ko‘rsatkichining sonli qiymatlarini tahlil qilish IoT trafikining hujumlar yo‘qligida fraktal xususiyatlarga ega emasligini, ammo OS Scan hujumi paydo bo‘lganda bu xususiyatlarning kuzatilishini ko‘rsatadi, bu esa aniqlash algoritmi yaratish asosi bo‘lishi mumkin.

Bu hodisani IoT qurilmalarining trafik xususiyatlari bilan tushuntirish mumkin. Mirai hujumi kabi, OS Scan hujumi Hurst ko‘rsatkichining joriy bahosi H chegaraviy darajasidan oshganda ishonchli ravishda aniqlanishi mumkin (5d-rasmga qarang). SSDP Flood hujumi uchun ham o‘xshash natijalar kuzatiladi. Hurst ko‘rsatkichining sonli qiymatlari (11) va (12) algoritmlaridan foydalanilganda 5e va 5f rasmlarda keltirilgan.

5-rasmda keltirilgan bog‘liqliklarni taqqoslash tahlili shuni ko‘rsatadiki, hujumlar FR baholash uchun eng yaxshi natijalarni (12) algoritmi ko‘rsatadi, bu algoritm thresholding (chegaraviy qiymatlash) shaklida qo‘shimcha filtrlash bilan amalga oshirilgan wavelet-tahlilga asoslangan joriy FR baholash usulini amalga oshiradi.

Xulosa. Tadqiqot natijasida IoT tarmog‘ining tasvirlangan topologiyasidagi turli nuqtalarda va har xil turdagi hujumlar uchun normal trafikning fraktal o‘lchamligi statistik parametrlari aniqlandi. IoT trafikining o‘z-o‘ziga o‘xshashlik xususiyatlariga ega bo‘lishi mumkinligi haqida xulosa qilish mumkin, agar tarmoqqa kiruvchi qurilmalar oddiy tarmoqlar uchun odatiy bo‘lgan stasionar kompyuterlar va mobil qurilmalar kabi qurilmalardan iborat bo‘lsa. Biroq, agar kompyuter tarmog‘i faqat past to‘plash qobiliyatiga ega IoT qurilmalaridan iborat bo‘lsa, trafikning fraktal xususiyatlari yo‘qoladi. Shu bilan birga, OS Scan va SSDP Flood turidagi hujumlarga duch kelganda, tahlil qilingan trafikda fraktal xususiyatlar kuzatiladi, bu esa IoT tarmoqlaridagi kompyuter hujumlarini aniqlash algoritmlarini yaratishda foydalanish mumkin bo‘lgan faktor hisoblanadi. Onlayn tarzda tarmoq trafikini tahlil qilishda esa FR baholash uchun modifikatsiya qilingan Hurst ko‘rsatkichini baholash algoritmi, ya’ni analiz oynasida sirpanib yuruvchi (12) usuli va chegaraviy qiymatlashdan foydalanish afzalroqdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT). Telecom Italia S.p.A.; 2015. p.10–21.
2. Dorsemaine B., Gaulier J.-P., Wary J.-P., Kheir N., Urien P. Internet of Things: A Definition & Taxonomy. Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST, Cambridge, UK, 09–11 September 2015). IEEE: 2015. DOI:10.1109/NGMAST.2015.71

3. Statista. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide [Accessed 12.02.2023].
4. Securelist. Demeter D., Preuss M., Shmelev Y. IoT: a malware story. 2019. URL: https://securelist.com/iot-a-malwarestory/94451 [Accessed 11.02.2023].
5. Shevtsov V.Y., Kasimovsky N.P Threat and vulnerability analysis of IoT and IIoT concepts. NBI technologies. 2020;14(3): 28–35. DOI:10.15688/NBIT.jvolsu.2020.3.5
6. Sheluhin O. I. Network Anomalies. Detection, Localization, Forecasting. Moscow: Goryachaya liniya – Telekom Publ.; 2019. 448 p.
7. Sheluhin O.I., Osin A.V., Smolsky S.M. Self-Similarity and Fractals. Telecommunication. Moscow: Fizmatlit Publ.; 2008. 368 p.
8. Sheluhin O.I., Lukin I.Yu. Network traffic anomalies detection using fixing method of jumps of multifractal dimension in the real-time mode. Automatic Control and Computer Sciences. 2018;52(5):421–430. DOI:10.3103/S0146411618050115.
9. Sheluhin O., Rybakov S., Vanyushina A. Modified Algorithm for Detecting Network Attacks Using the Fractal Dimension Jump Estimation Method in Online Mode. Proceedings of Telecom. Univ. 2022;8(3):117–126. DOI:10.31854/1813-324X-2022-8-3-117-126.
10. Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode. Proceedings of the Conference on Wave Electronics and its Application in Information and Telecommunication Systems. WECONF, 30 May – 03 June 2022, St. Petersburg, Russia. IEEE; 2022. DOI:10.1109/WECONF 55058.2022.9803635.
11. Sheluhin O.I., Rakovskiy D.I. Multi-Label Learning in Computer Networks. Proceedings of the Conference on Systems of Signals Generating and Processing in the Field of on Board Communications, 14–16 March 2023, Moscow, Russia. IEEE; 2023. DOI:10.1109/IEEECONF56737.2023.10092157.
12. Bolshakov A.S., Gubankova E.V. Anomaly detection in computer networks using machine learning methods. REDS: Telecommunication Devices and Systems. 2020;10(1):37–42.
13. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. arXiv:1802.09089. 2018. DOI:10.48550/arXiv.1802.09089.
14. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi, et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features. Proceedings of the Second International Conference on Intelligent Systems and Pattern Recognition, ISPR 2022, 24–26 March 2022, Hammamet, Tunisia. Communications in Computer and Information Science, vol.1589. Cham: Springer; 2022. p.306–314. DOI:10.1007/978-3-031-08277-1_25.
15. Alabdulatif A., Rizvi S.S.H. Machine Learning Approach for Improvement in Kitsune NID. Intelligent Automation & Soft Computing. 2022;32(2):827–840. DOI:10.32604/iasc.2022.021879.